IT Unit 3

Topic 1

# Organisations & Data Management

**Protecting valuable data, p 57**

1. Why is it important that stored data is kept secure?

* Unprotected data is a liability for a business, any entities need to keep data secure so it’s protected and safe. If data is stolen it could mean the end of a business cause if personal and finance information gets out about people, they don’t be happy.

1. What are the 2 types of controls that can protect data?

* By either using hardware or software

Measures to protect data:

Physical equipment controls include zoned security strategies, barrier techniques and biometrics.

A What is meant by biometrics and what is its advantage as a means of protecting data?

* Biometric simple means using a single person to protect a device. For example, on all current iPhone there a feature that use one of your single finger or thumbs scan and keeps that information is a protection. So every time this phone was use you would need the person figure print

1. Backing up
   1. What are the 3 types of backing up?

* Full back up: copies all of the fillies from devices to a storage medium.
* Differential backup: copies only those fillies that have been charge since the last full backup.
* Incremental backup: is similar to a differential back, the difference being that it uses more than two media.
  1. List some backup options?
* Many databases support version control of data, so they actually store changes to each data element in any record so that if necessary only that particular fields are restored

1. Electrical protection
   1. What is the role of a UPS?

* Uninterruptable power supply (UPS) can regulate electricity coming into a computer and supply back up electricity for a short time if there a black out.

1. Usernames & passwords
   1. What are the characteristics of a good password?

* At least 8 characters containing a mix of letter and number being camel case
  1. What is the role of access logs, audit trails and access restrictions?
* access log is a list of all the requests for individual files that people have requested from a Website Systems security software.
* Audit trails are records of any change to a database
* Access restriction is just simply not having access to certain areas on a database which requires manger access 0r something.
  1. What types of security software should organisations run?
* Firewalls, malware
  1. Explain the nature of malware and phishing software
* Malware: software which is specifically designed to disrupt, damage, or gain authorized access to a computer system.
* Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details.
  1. Explain the nature of a firewall?
* A firewall is a [network](http://searchnetworking.techtarget.com/definition/network) security system, either hardware- or software-based, that uses rules to control incoming and outgoing network traffic.

1. Encryption
   1. What does encryption involve?

* the process of converting information or data into a code, especially to prevent unauthorized access.
  1. What protocols are used for encryption?
* https, SQL
  1. What is hashing?
* hash function which takes an input (or 'message') and returns a fixed-size alphanumeric string.